How To Use Firefox Privacy Settings to Make Your Browsing Secure

Juliana Kenny, Author Catherine McNally, Editor

Last updated Aug 24, 2023

We may receive compensation from the products and services mentioned in this story, but the opinions are the author's own. Compensation may impact where offers appear. We have not included all available products or offers. Learn more about how we make money and our editorial policies.

While Firefox provides decent privacy and security features, out of the box, its default settings prevent it from being considered a private browser. With some modifications to its settings and the addition of certain add-ons, Firefox's security improves considerably — making it comparable and competitive with other private browsers.

Keep reading to find out which privacy settings you should change to improve your Firefox browser's anonymity as well as which add-ons, including the best VPNs and ad blockers, to use with your browser.

In this article

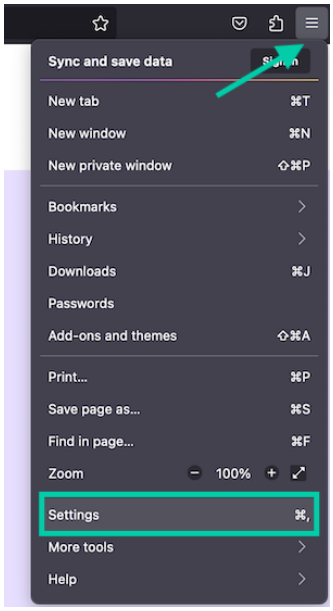
5 Firefox privacy settings to change for online anonymity

1. Change your default search engine

One of the simplest steps you can take to increase your browsing privacy is to change the search engine Firefox uses by default to a private search engine.

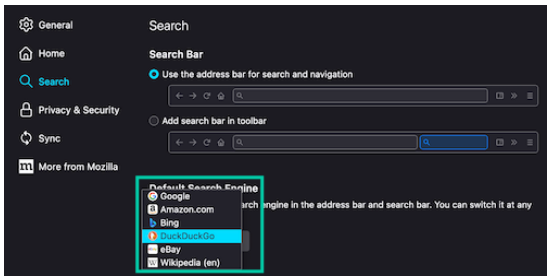
As far as free private search engines go, DuckDuckGo is easy to use and never stores or tracks any personal information. You're essentially browsing anonymously when using it. Here's how to set your default search engine to DuckDuckGo in Firefox:

1. Open the Firefox application menu, located in the top-right corner of your browsing screen by clicking the three horizontal lines. Navigate to and click Settings.



2. Click Search in the left menu.

3. Find the section labeled “Default Search Engine,” click the dropdown menu, and select DuckDuckGo from the list of options.



2. Set up Enhanced Tracking Protection (formerly known as Content Blocking)

Enhanced Tracking Protection is Firefox’s native malware and tracker-blocking tool. By default, Enhanced Tracking Protection blocks the following:

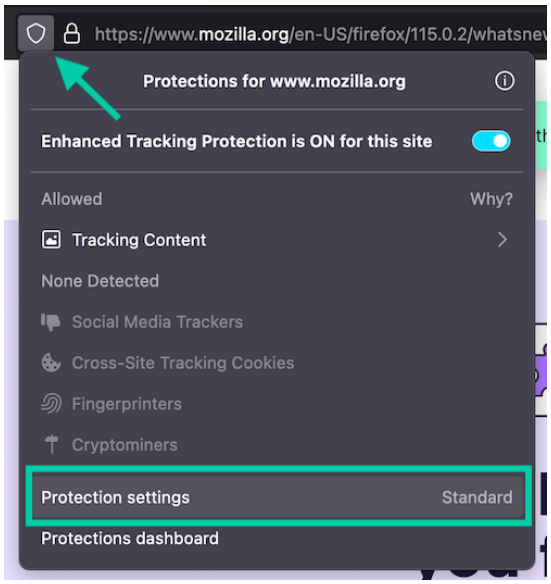
- Cryptominers
- Social media trackers
- Fingerprinters
- Cross-site tracking cookies
- Tracking content

Enhanced Tracking Protection comes in three modes: Standard, Strict, and Custom, and it’s set to Standard by default. Users should be aware that in Standard mode, tracking content will be blocked only while using Private Windows. Thus, users looking for more protection will need to manually adjust Firefox’s Privacy & Security settings.

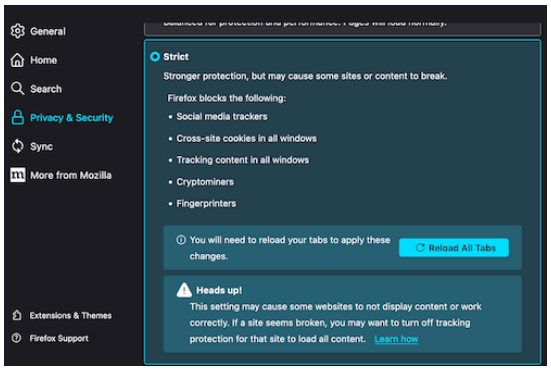
To change Enhanced Tracking Protection from Standard to Strict, do the following:

1. Click the shield icon located on the left side of the address bar.

2. In the dropdown menu, click “Protection Settings.” It should read “Standard” on the right side.



3. Click the toggle labeled “Strict.”


General
Home
Search
Privacy & Security
Sync
More from Mozilla
Extensions & Themes
Firefox Support
Strict
Stronger protection, but may cause some sites or content to break.
Firefox blocks the following:
• Social media trackers
• Cross-site cookies in all windows
• Tracking content in all windows
• Cryptominers
• Fingerprinters
You will need to reload your tabs to apply these changes.
Reload All Tabs
Heads up!
This setting may cause some websites to not display content or work correctly. If a site seems broken, you may want to turn off tracking protection for that site to load all content. Learn how

4. Users looking for more control over what Firefox blocks, can instead enable Custom mode in which they may manually enable or disable security features as they desire.

> Note: Strict Enhanced Tracking Protection may cause certain websites to display or function improperly.

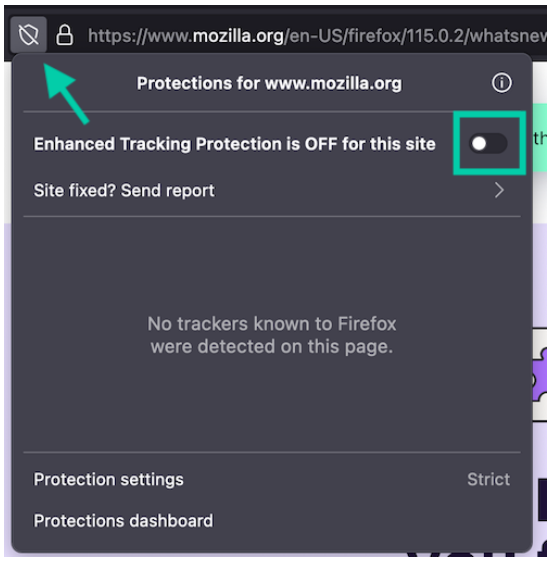
What should I do if Enhanced Tracking Protection breaks a website?

If a website is malfunctioning, you can easily toggle Enhanced Tracking Protection off for that specific website by doing the following:

1. Click the shield icon located on the left side of the address bar.

2. Click the toggle labeled Enhanced Tracking Protection is ON for this site.

3. The web page should reload automatically, and Enhanced Tracking Protection will be off for that site only.



3. Toggle on “Do Not Track”

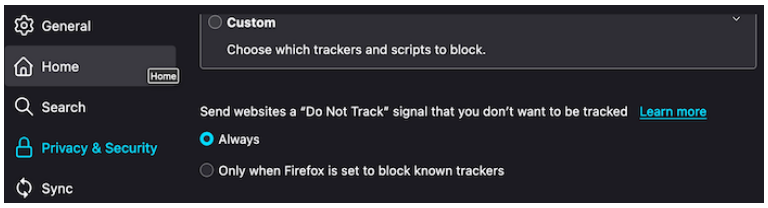
Most websites track your behavior in order to store and sell that information to other companies for advertising purposes. This means even if you’re using a private search engine, websites you visit may still try to store your personal information.

Firefox has a privacy setting that sends a Do Not Track signal to websites you visit. To toggle on Do Not Track in Firefox, do the following:

1. Click the menu button represented by the three horizontal lines in the upper-right corner of your browsing window and then click Settings.

2. Select Privacy & Security from the menu on the left of the screen.

3. Find the section labeled “Send websites a ‘Do Not Track’ signal that you don’t want to be tracked” and click the toggle to Always.


General
Home
Search
Privacy & Security
Sync
Custom
Choose which trackers and scripts to block.
Send websites a "Do Not Track" signal that you don't want to be tracked Learn more
Always
Only when Firefox is set to block known trackers

Note: Websites aren't required to honor the Do Not Track request, so while we still recommend this setting in Firefox, it shouldn't be your primary source of privacy protection.

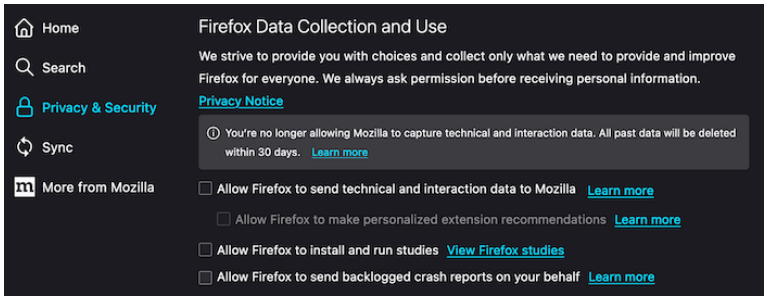
4. Disable Firefox telemetry

Firefox collects telemetry data by default in order to improve its stability and performance. Telemetry data exists in two forms: interaction data and technical data.

- **Interaction data** consists of information centered around your interactions with Firefox, such as the number of webpages visited, number and type of installed add-ons, number of open tabs and windows, and session length.
- **Technical data** pertains to information such as the operating system and device hardware you're using, the version of Firefox and language you're using, information about errors and crashes, and update and safebrowsing logs.

In addition to all of the above, your IP address is sent to Firefox and stored for 14 days when telemetry data is collected. If you're concerned about your privacy, you should opt out of telemetry data collection by doing the following:

1. Click the menu button represented by the three horizontal lines in the upper right corner of your browsing window and then click Settings.
2. Select Privacy & Security located in the menu on the left of the screen.
3. Scroll down to the section labeled "Firefox Data Collection and Use."
4. Disable the box labeled "Allow Firefox to send technical and interaction data to Mozilla."

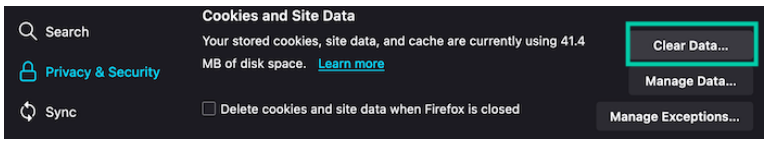

Home
Search
Privacy & Security
Sync
More from Mozilla
Firefox Data Collection and Use
We strive to provide you with choices and collect only what we need to provide and improve Firefox for everyone. We always ask permission before receiving personal information.
Privacy Notice
You're no longer allowing Mozilla to capture technical and interaction data. All past data will be deleted within 30 days. Learn more
Allow Firefox to send technical and interaction data to Mozilla Learn more
Allow Firefox to make personalized extension recommendations Learn more
Allow Firefox to install and run studies View Firefox studies
Allow Firefox to send backlogged crash reports on your behalf Learn more

When you opt out of telemetry data collection, Firefox treats it as a request to delete previously collected data, which they claim to do within 30 days of opting out.

5. Clear your cookies and cache

When you browse websites, Firefox stores data such as scripts and images to speed up loading times. It even keeps you logged into accounts for a smoother browsing experience. Clearing Firefox cookies and cache manually takes only a few moments and can help keep your browsing history and online accounts secure. To clear cookies and cache, do the following:

1. Click the menu button represented by the three horizontal lines on the upper right side of your browser window and select Settings.
2. Choose Privacy & Security and scroll down to the section labeled "Cookies and Site Data." s
3. Select the Clear Data button.
4. Select Clear in the window that opens.

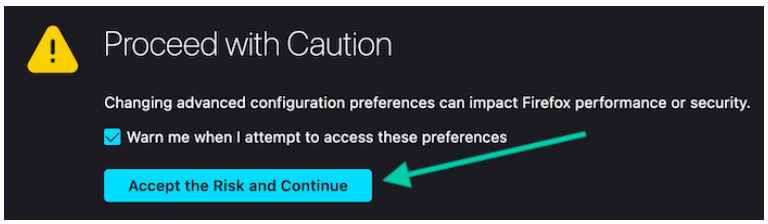

Search
Privacy & Security
Sync
Cookies and Site Data
Your stored cookies, site data, and cache are currently using 41.4 MB of disk space. Learn more
Clear Data...
Manage Data...
Manage Exceptions...
Delete cookies and site data when Firefox is closed

Note: If you'd like to remain logged into your accounts, uncheck the box next to "Cookies and Site Data" before clicking the Clear button.

7 advanced Firefox privacy settings

There are a number of more advanced settings you can adjust to increase Firefox security. However, these modifications require using commands, and — if done incorrectly — could damage Firefox. We recommend only advanced users consider these settings.

To open Firefox's advanced privacy settings, type **about:config** in the web address bar and hit enter. Click Accept the Risk and Continue in the warning window that opens. A new window will open in Firefox with a search bar at the top of the screen into which you can enter commands.


Proceed with Caution
Changing advanced configuration preferences can impact Firefox performance or security.
Warn me when I attempt to access these preferences
Accept the Risk and Continue

1. Disable WebRTC

Web Real-Time Communication — or WebRTC — allows P2P sharing, video chat, and voice in your browser, but it can also expose your IP address through a WebRTC leak.

Disable WebRTC in Firefox by entering **media.peerconnection.enabled** into the advanced settings search bar. Then double-click the double arrows to change it to read "False."

2. Block browser fingerprinting

Fingerprinting refers to another form of online tracking that uses your device hardware, software, preferences, add-ons, and even installed fonts to create a unique profile for you. This allows companies to track you for months — even when applying best security practices like using private browsing mode or clearing your browsing storage.

Firefox's Enhanced Tracking Protection currently protects against certain types of fingerprinting. To further harden Firefox's protection to other types of fingerprinting, we recommend turning on resist fingerprinting.

Turn on resist fingerprinting

Type **privacy.resistFingerprinting = true** into the advanced settings search bar and hit enter. You will be provided with a result under the search bar with a + sign to the right of the result.

Leave the toggle in the middle set to Boolean and click the + button on the right side of the result so the value reads "true" in the center.

Block cryptominers

Type **privacy.trackingprotection.cryptomining.enabled = true** into the advanced settings bar and follow the same steps as above to make the value read "true."

3. Turn on privacy tracking protection

Type **privacy.trackingprotection.enabled = true** into the advanced setting bar, following the same steps above to make the value read "true."

4. Disable geolocation tracking

Type **geo.enabled = false** into the advanced settings bar and follow the same steps as above, keeping the toggle set to Boolean. This time, click the + button on the right until it reads "false" in the center of the result.

5. Disable tracking cookies

Type **network.cookie.cookieBehavior** into the advanced settings bar. This setting is an integer type where different values denote different cookie preferences. The value preferences are as follows:

- 0 = Accept all cookies by default (not recommended for security)
- 1 = Only accept cookies from the originating site (block third-party cookies)
- 2 = Block all cookies by default
- 3 = Block cookies from unvisited sites
- 4 = New Cookie Jar policy (prevent storage access to trackers)

Double-click the pencil button next to **network.cookie.cookieBehavior** in your results, type in the value you want, and press enter. Values 1–4 offer increasing amounts of privacy; however 4 can prevent certain websites from functioning properly.

6. Turn off microphone and camera tracking

Type **media.navigator.enabled = false** into the advanced settings bar, keeping the value set to Boolean and clicking the + button on the right side of the value until it reads “false” in the center.

7. Turn off clipboard tracking

Type **dom.event.clipboardevents.enabled = false** into the advanced settings bar, keeping the value set to Boolean and clicking the + button on the right side of the value until it reads “false” in the center.

3 Firefox add-ons for more online privacy

Firefox add-ons are a great way to further secure your privacy. Below are some common and popular add-ons worth considering.

1. Virtual private network (VPN)

A VPN is a service that secures the connection between your device and the internet by masking your real IP address and encrypting your internet activity. When your VPN is active it’s harder to track your location and online behavior. VPNs also allow you to bypass content blocking and censorship.

Below we discuss the three best VPN services we recommend.

- **Surfshark:** Surfshark VPN is a great budget-friendly option (starting as low as $2.49/mo) that protects an unlimited number of devices — making it even more desirable for families or large households. You’ll need to pay extra for Surfshark Antivirus, but its VPN does come with CleanWeb, an ad and malware blocker.

  Get Surfshark | Read Our Surfshark Review

- **NordVPN:** NordVPN is a well established and easy-to-use VPN that offers a wide array of features, including built-in antivirus tools. It comes in a little pricier than other VPNs (starting at $3.49/mo), but its well-polished and professional-grade service is well worth it.

  Get NordVPN | Read Our NordVPN Review

- **ExpressVPN:** ExpressVPN comes in as one of the more expensive VPN services (starting at $8.32/mo), but it seems to make up for that price hike in the protection and quality of life it provides. Described as a VPN you can “set and forget,” ExpressVPN gives users access to content everywhere with server locations in 94 countries — making it a great VPN option for those who regularly see content censorship as a result of where they live.

  Get ExpressVPN | Read Our ExpressVPN Review

Surfshark®

★★★★★ 4.9

Limited-time offer: 82% off + 4 months free

Surfshark

Learn More →

On Surfshark's website

- VPN technology offering stability and speed
- Unlimited simultaneous connections
- Works with Netflix and other streaming services
- Headquarters in Nine Eyes Alliance

2. Ad blocker

Ad blockers are software designed to remove advertisements from websites. A convenient feature of ad blockers is that they also increase user security and privacy. This is because malware tends to be hidden in pop-up ads, and third parties use advertising trackers to spy on your internet activities.

Below is a list of popular and useful ad blockers we recommend.

- **Total Adblock:** TotalAdblock is a great option if you're looking for a complete security package — its premium version comes with TotalAV antivirus protection.

  Get Total Adblock | Read Our Total Adblock Review

- **Ghostery:** Ghostery is known for its well-designed user interface and for providing information regarding how you're being tracked and what Ghostery is currently blocking. You can get a lot out of the free version of Ghostery, while the paid version includes historical stats, extension themes, and more.

  Get Ghostery | Read Our Ghostery Review

- **uBlock Origin:** A free and open-source product, uBlock Origin provides the protection you expect out of an ad blocker while minimizing its impact on CPU and memory usage. It also provides tools aimed at advanced users, such as the dynamic filtering tool, allowing deeper customization of security options.

  Get uBlock Origin | Read Our uBlock Origin Review

TOTAL Adblock

4.5

Limited-time offer: 80% off

Learn More →

On Total Adblock's website

Total Adblock

- Remove ads & trackers on YouTube, Facebook, and most websites
- Hands-off ad-blocking experience
- Easy to set up
- Free version excludes top 15,000 websites

3. Password manager

Password managers store, manage, and protect your login credentials, making it easier for you to have strong and varied passwords without needing to rely on memorization. So much of our sensitive personal information is linked to accounts protected by our passwords, so we highly recommend password managers for users looking to boost their online security.

Below is a list of what we've found to be the best Firefox password managers.

- **NordPass:** With its easy-to-use interface and good range of security features, NordPass is a solid beginner-friendly password manager. Additionally, its free version includes all of its core features and can be linked to an unlimited number of devices. (But it's valid only for one account.)

  Get NordPass | Read Our NordPass Review

- **1Password:** 1Password is a premium-only password manager with personal plans starting at $2.99/mo. While 1Password might be on the pricier end of the spectrum, it offers high-end security options for individuals, families, and businesses alike.

  Get 1Password | Read Our 1Password Review

- **Bitwarden:** Bitwarden is an open-source password manager that allows you to access and contribute to its development. Its free version comes with all of its core features — including multi-device sync and unlimited items in your vault — while its paid plans start at about 83 cents/mo.

  Get Bitwarden | Read Our Bitwarden Review

NordPass®

5.0

Limited-time offer: 56% off + 3 extra months

Learn More →

On NordPass's website

NordPass

- Strong encryption and security
- User-friendly interface
- Free version is limited to one device at a time

3 browser alternatives safer than Firefox

Firefox can be a safe browser but requires some modifications in order to be optimally secure. There are other browsers that compete with or even surpass Firefox in terms of security and privacy. Here are a few free browsers worth checking out:

1. Tor Browser

Tor Browser is an open-source browser that provides private browsing without tracking, surveillance, or censorship. Its privacy features are competitive with Firefox's, however, it's known to produce slower browsing speeds than its competitors and some of its security features aren't beginner friendly. If you're an advanced user and want to support open-source, volunteer-run software, Tor Browser may be for you.

2. Epic Privacy Browser

Epic Privacy Browser acts similarly to a VPN because it hides your IP address and encrypts your internet traffic out of the box. It's essentially akin to permanently browsing in "private browsing" mode. While you can do some tinkering to get Epic Privacy Browser working at its full potential, its default settings are centered around extreme privacy, making it a good option if you want high security without too much setup.

3. Brave Browser

Brave Browser is a good option if you're looking for extra security options without sacrificing performance. Brave downloads only essential elements of websites while blocking ads and trackers, resulting in much faster load times. It also offers VPN and Firewall services for $9.99 a month or $99.99 a year.

How to make Firefox private FAQs

Is Firefox safe for privacy?

Out of the box, Firefox is good for privacy, but it's not perfect. With some light modifications and some advanced tweaking, Firefox can be a very safe browser.

How do I make Firefox more private and secure?

The simplest and quickest ways to make Firefox more private and secure would be to:

1. Change your default search engine to a private search engine, such as DuckDuckGo.
2. Set Enhanced Tracking Protection to Strict.
3. Clear cookies and cache.
4. Disable Firefox Telemetry.
5. Toggle on "Do Not Track."

How do I clear my browsing history in Firefox?

1. Click the menu button in the top right corner of your browser represented by the three horizontal lines and click “Settings.”
2. Select “Privacy & Security” from the menu on the left.
3. Scroll down to the section labeled “History” and click the button labeled “Clear History.”
4. Select a time range to clear in the drop-down list and toggle what information you want to clear. Click “Clear Now.”

Bottom line

Firefox performs well in terms of privacy but still requires some adjustments for optimal security. **Add-ons such as VPNs, password managers, and ad blockers shouldn’t be overlooked by Firefox users looking for the highest level of privacy and security.**

And if privacy is a concern of yours and you want to prevent online tracking, check out our best ad blockers review to find out which ad blocker is right for you.

NordVPN®

4.9

Limited-time offer: 69% off + 3 extra months

Learn More →

On NordVPN's website

NordVPN

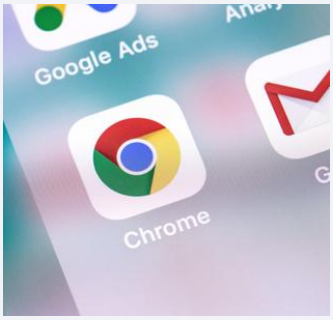
- High-quality VPN offering safety and speed
- Loads of servers for multiple connection options
- Works with popular streaming services, including Netflix
- Too many confusing plans

Author Details

Juliana Kenny
About the Author

Juliana Kenny is a freelance writer with 13 years of experience specializing in cybersecurity topics. Her expertise includes endpoint security, cloud security, and networking technologies like secure access service edge (SASE). She has written for technology giants, including Oracle, Hitachi Vantara, and Comcast. When she's not diving deep into security news, you can find her bird-watching or baking.

Related Articles



Malwarebytes Antivirus Review 2023: Is It Worth the Hype?

Malwarebytes is a user-friendly antivirus option, but does it have everything you need? Find out if this popular program is right for you.

What is a VPN and Why Would You Use One?

Learn what a VPN is and why you might want to use one for secure and encrypted internet connections.

How To Clear Cookies On Your Google Chrome Browser

When you use Google Chrome, it saves information from the websites you visit. Clearing these files, called cookies, may fix some of your computer issues. Here's how to do it.

How To Browse Online Without Anyone Knowing

Here's how a VPN, secure browser, encrypted email, and other tools can help protect your anonymity while browsing the internet.

Copyright © 2023 **All About Cookies**
111 E. Atlantic Ave., Suite 200
Delray Beach, FL 33444

All About Cookies is an informational website that provides tips, advice, and recommendations to help you with Online Privacy, Identity Theft Prevention, Antivirus Protection, and Digital Security. We strive to provide up-to-date information, but make no warranties regarding the accuracy of our information. Ultimately, you are responsible for your digital security. All About Cookies is not a digital security product and does not provide any digital security products.